U. S. Department of Justice

United States Attorney
Northern District of Illinois

Patrick J. Fitzgerald
United States Attorney

Federal Building
219 South Dearborn Street, Fifth Floor
Chicago, Illinois 60604
(312) 353-5300

FOR IMMEDIATE RELEASE
WEDNESDAY FEBRUARY 1, 2006
www.usdoj.gov/usao/iln

PRESS CONTACT:
AUSA Pravin Rao (312)353-1457
AUSA/PIO Randall Samborn (312) 353-5318

19 INDICTED IN $6.5 MILLION "RISCISO" SOFTWARE PIRACY CONSPIRACY

CHICAGO – Nineteen defendants from across the United States and overseas who allegedly were leaders, members and associates of the underground software piracy group known as "RISCISO" were indicted on federal charges for pirating more than $6.5 million of copyrighted computer software, games, and movies through non-public Internet sites. The defendants were charged in a 15-count indictment that was returned late yesterday by a federal grand jury in Chicago, where the investigation was conducted, Patrick J. Fitzgerald, United States Attorney for the Northern District of Illinois, and Robert D. Grant, Special Agent-in-Charge of the Chicago Office of the Federal Bureau of Investigation, announced today.

The charges stem from an undercover investigation of RISCISO, an online "warez" organization, founded in approximately 1993, dedicated to illegally distributing newly-released copyrighted software, games and movies. "RISC" was an acronym for Rise in Superior Couriering, while "ISO" referred to a file format commonly used for the storage and transfer of pirated software. RISCISO allegedly was a sophisticated warez "release" group that operated until last summer as an original source for thousands of pirated works, with over 19,000 gigabytes (equivalent to more than 23,000 CD ROMs) uploaded and downloaded on one server alone via the Internet.

The copyrighted works included operating systems, utilities, word processing, data analysis and spreadsheet applications, communications programs, graphics, desktop publishing and games that could be played on computers and on video gaming consoles such as Xbox and Playstation 2.

The Chicago investigation, code-named *Operation Jolly Roger*, was one of three separate undercover operations – the other two were based in Charlotte and San Jose – that were part of a coordinated international law enforcement initiative known as Operation Site Down, which was announced by the Justice Department last summer.

Starting in late 2003, a cooperating witness (CW) in the Chicago investigation maintained one of the computer servers that hosted RISCISO's alleged Internet distribution of copyrighted materials, giving FBI agents access to tracking the illegal computer trafficking activity. Together with the 2001 prosecution of nine defendants who were associated with the software piracy group known as "Fastlane," this investigation marks the second successful infiltration of a warez group by the FBI in Chicago.

"Online thieves who steal merchandise that companies work hard to produce and protect might think that cyberspace cloaks them in anonymity and makes them invulnerable to prosecution, but we have the ability to infiltrate their secret networks and hold them accountable for their criminal conduct," Mr. Fitzgerald said. "Intellectual property deserves protection by law enforcement just like any other property," he added. Mr. Grant said: "Our repeated success at this type of sophisticated and technically complex investigation shows that the FBI is able to collect evidence enabling us to identify, locate and prosecute alleged cybercriminals anywhere in the world. There is no refuge for computer crime in cyberspace."

The undercover phase of the investigation ended on June 29, 2005, when FBI agents executed approximately 70 search warrants nationwide and 20 more in 10 foreign countries as part of the Chicago, Charlotte and San Jose-based operations.

All 19 defendants were charged with one count of conspiracy to commit copyright infringement, and 15 of the 19 were charged with one additional count each of copyright infringement. The indictment also seeks forfeiture of 172 items of computer hardware and related electronics that were seized from the defendants during the searches. The defendants are:

Sean Patrick O'Toole, 26, also known as "chucky," of Perth, Australia; allegedly the defacto leader of RISCISO, who set policy for the group, decided who had access to the servers, and uploaded copyrighted material from remote sites he personally controlled;

Vahid Pazirandeh, 25, aka "vman," of San Diego; a former university employee, who allegedly held a leadership role in RISCISO and served as a site operator responsible for establishing, maintaining, administering, and supporting many of the group's warez servers;

Linda Waldron, 57, aka "bajantara," of Barbados;

Paul Yau, 32, aka 'ann," Houston;

Sandy Fury, 39, aka "asylum," of West Hollywood, Ca.;

Marc Bartel, 33, aka "biosprint," of Overland Park, Ks.,

Tu Nguyen, 29, aka "dray," of Chicago;

Richard Balter, 46, aka "ducky," of Middle Island, N.Y.;

Danny Lee, 31, aka "messy," of Rosemead, Ca.;

Peter Andrew Holland, 22, aka "thebinary," of Middletown, Oh.;

Jason Dobyns, 26, aka "supafly," of Tustin, Ca.;

David Lewis, 33, aka "keymaster," of Costa Mesa, Ca.;

Matthew Cittell, 27, aka " keymaster," of Costa Mesa, Ca.;

Matthew Ploessel, 24, aka " kkits" and "stikk," of Seattle;

Joseph Toland, 44, aka "anim8," of Rochester Hills, Mi.**;**

Fred Amaya, 41, aka "audiovox," of Chino Hills, Ca.;

Lance Warner, 29, aka "transform," of Portola Hills, Ca.;

Gregg Piecyhna, 51, of New York City; and

Jeremiah Stevens, 27, aka "^mort^," of Jasper, In.

According to the indictment, a number of the defendants were employed in high-tech industries. The defendants include information technology directors for a law firm, an architectural firm, and a telecommunications company; two systems administrators for Internet service providers; the owner of a computer security company; a software consultant and mathematics doctoral candidate; and an employee of a company that provided software services to the United States Navy. All 19 defendants will be ordered to appear for arraignment at a later date in U.S. District Court in Chicago.

According to the indictment, between 1998 and June 29, 2005, in exchange for their contributions of hardware or pirated works, members and associates of the RISCISO conspiracy received access through the Internet to computers that stored extensive libraries of illegally copied copyrighted software, games and movies. (The computers used to maintain these libraries were referred to as "warez sites" or "warez servers.") RISCISO members set up computer servers that hosted warez sites used to store and distribute copyrighted software, games and movies, and some members of the conspiracy devoted substantial time and resources to RISCISO-related activities. From 1998 through 2003, RISCISO members surreptitiously set up a warez servers, each known as RM1 or RM2, at computer facilities located in Los Angeles, Kansas and Houston.

In December 2003, RISCISO members started using a new RM2 server, which was administered by Pazirandeh, who also provided some of its hardware components and installed the operating systems, firewalls, and encryption programs necessary to operate and protect the server from detection. Unbeknownst to the defendants, however, the computer hosting the RM2 server was maintained by the CW, who was assisting the government's investigation of RISCISO, according to the indictment. It alleges that the CW was given physical and root access to the RM2 server by O'Toole. By 2004, RM2 was RISCISO's main server.

As part of the conspiracy, in September 2003, Pazirandeh allegedly sent a computer server and 17 computer hard drives to the CW for use in building the RM2 server. This hardware was originally used in RISCISO's Los Angeles RM1 server. In March and June 2004, Amaya also allegedly sent, first, three SATA hard disk drives and, later, a SATA Raid Controller card to the CW for use in the RM2 server.

During the time that RM2 was in operation, RISCISO members who were allowed access by O'Toole, Pazirandeh and others allegedly uploaded and downloaded 19 terabytes – or 19,000 gigabytes – of software, games and movies with a total retail value in excess of $6.5 million. In the six months prior to April 2005, the pirated content included:

> software such as Ulead Picture Show 3 Deluxe, Microsoft Windows XP Media Center Edition 2005, Microsoft Streets and Trips 2005, Cakewalk Sonar4 Producer, Ahead Nero Burning Rom Version 6.6 Ultra Edition, Autodesk Mechanical Desktop Version 2006, Windows XP Pro 64-bit, Intel Fortran Compiler Version 8.1, Husqvarna Viking 3D Embroidery System, Hewlett-Packard Openview Network Node Manager Version 7.5, Roxio Easy Media Creator Version 7.5 and Windows Server 2003 Enterprise VL Edition;
>
> movies such as Sideways, The Pacifier, The Aviator, Closer, The Incredibles, Meet the Fockers, Hostage, Vanity Fair, Oceans 12, Spanglish, Shark Tale, Alexander, The Phantom of the Opera, Sin City, Flight of Phoenix, Collateral, and Robots; and

games such as Tiger Woods PGA Tour 2005, Half Life 2, Tony Hawk's Underground 2, Tribes Vengeance, Super Streetfighter II, NASCAR Simracing, and WW II Sniper.

As part of the conspiracy, the defendants and other members of RISCISO allegedly employed sophisticated security measures to conceal their activities, communications, and identities from law enforcement, and to ensure that only persons authorized by the leaders of RISCISO could gain access to the millions of dollars worth of software, movies, and games stored on its servers. They communicated with each other on private Internet Relay Chat (IRC) channels, such as "#risciso and #dvdiso, and access to their warez sites was carefully limited to authorized users entering through known Internet Protocol addresses with pre-established IDs and passwords. To conceal their activities, the defendants used "drop sites" – computers ordinarily located outside the United States and not easily associated with individual RISCISO members, screen names instead of true names and port bouncers to disguise the true Internet Protocol addresses of their computers and the computers that hosted the warez sites, according to the indictment.

The conspiracy and copyright infringement charges in this case were brought under the No Electronic Theft Act, known as the NET Act, which enables prosecutions of copyright piracy. The NET Act makes it illegal to reproduce or distribute copyrighted works, such as software, games and movies, even if the defendant acts without a commercial purpose or for private financial gain.

The government is being represented by Assistant U.S. Attorneys Pravin Rao and Angela Crawford. The Justice Department's Computer Crime and Intellectual Property Section, which is part of the Department's Criminal Division, has provided assistance.

If convicted, conspiracy to infringe a copyright carries a maximum penalty of five years in prison and a $250,000 fine, and copyright infringement carries a maximum of three years in prison

and a $250,000 fine. Restitution is mandatory. The Court, however, would determine the appropriate sentence to be imposed.

The public is reminded that an indictment contains only charges and is not evidence of guilt. The defendants are presumed innocent and are entitled to a fair trial at which the government has the burden of proving guilt beyond a reasonable doubt.

# # # #